



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/847,037

04/30/2001

Brian T. Murren

GE1-003US

5208

21718

7590

08/24/2006

LEE & HAYES PLLC  
SUITE 500  
421 W RIVERSIDE  
SPOKANE, WA 99201

EXAMINER

SON, LINH L D

ART UNIT

PAPER NUMBER

2135

DATE MAILED: 08/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/847,037	<b>Applicant(s)</b> MURREN ET AL.	
	<b>Examiner</b> Linh LD Son	<b>Art Unit</b> 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 02 June 2006.
- 2a) ☐ This action is FINAL.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1,4-19,21-27,29,30 and 35-42 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,4-19,21-27,29,30 and 35-42 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |   |   |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____   | 6) <input type="checkbox"/> Other: _____                                    |

### DETAILED ACTION

1. This Office Action is responding to the RCE received on 06/02/06.
2. Claims 2-3, 28, 31-34 are canceled.
3. Claims 1, 4-19, 21-27, 29-30, 35-42 are pending.

### *Response to Arguments*

4. Applicant's arguments filed 06/02/06 have been fully considered but they are not persuasive.
5. As per remark on page 15, Applicant argues that the amended limitation "wherein the business logic employs interaction-based definitions in which a component which performs the operation is defined by a series of request-response interaction definitions that can be satisfied to perform the operation" does not disclose in Andrew's invention. Examiner respectfully disagrees with the Applicant. As cited in the rejection below (Col 7 line 52 to Col 8 line 35) discloses in detail of a business logic operation wherein a client object 206 attempts to access the functionality of the server object. A wrapper contains a series of security interaction definitions of the object (Col 7:58-62). Once all the

Art Unit: 2135

security interaction is completed, the operation is carried out and completed.

Therefore, Andrew still discloses the amended claims.

***Claim Rejections - 35 USC § 101***

6. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1 and 4-7 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The language of the claims 1 and 4-7 consists solely of computer program, which is nonstatutory functional descriptive material. A system of computer program is also nonstatutory functional descriptive material. The language ("system", "pluggable security policy enforcement module", "business logic", and "the business logic processes requests submitted to the system") of the claims does not recite any computer hardware involvement. See 35 U.S.C. 101.

8. In addition, Claims 1-42 are also rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. As an exemplary claim 1, the language of the claim 1 conveys a business logic interacting with a pluggable security policy enforcement module to provide a solution by solving problem, which is lacking of a tangible result and practical application. The business logic can be a mathematical operation to calculate a result. Since the pluggable security policy module is only the constrain on how the result gets produced, the system of claim 1 is

Art Unit: 2135

clearly lacking of practical application. (See *State Street*, 149 F.3d at 1375, 47 USPQ2d at 1602, and *At&T*, 172 F.3d at 1358, 50 USPQ2d at 1451). In a scenario, the business logic is an operation to provide a solution solving a logistic problem, the solution to the problem is not a useful, tangible and concrete until the solution is in practice. The language of the claim does not convey such detail.

***Claim Rejections - 35 USC § 102***

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1, 4-19, 21-27, 29-31, and 33-42 are rejected under 35 U.S.C. 102(e) as being anticipated by Andrews et al, US Patent No. 6487665B1, hereinafter "Andrews". (Cited in PTO 892 dated 6/03/05)

11. As per claim 1:

Andrew discloses "Andrew discloses "A system comprising: a pluggable security policy enforcement module configured to be replaceable in the system and to provide different granularities of control for a business logic in the system, wherein, business logic processes requests submitted to the system, wherein the business logic contains problem solving logic that produces solutions for a particular problem domain" in (Col 7

Art Unit: 2135

lines 53-67, and Col 8 lines 25-50), "wherein the pluggable security policy enforcement module is configured to determine, for a particular granularity of control, whether to permit an operation, requested by a user based at least in part on a permission assigned to the user" in (Col 8 lines 25-50), and "wherein the business logic employs interaction-based definitions in which a component which performs the operation is defined by a series of request-response interaction definitions that can be satisfied to perform the operation" in (Col 7 line 52 to Col 8 line 35), and "wherein the different granularities of control comprise a plurality of sets of rules that can be replaced with each other without altering the business logic" in (Col 7 lines 60-67, Col 17 lines 42-65, and Col 11 lines 30-60 (A set of rules associates with each role of many roles. For instance, the user can call the method and can also control access at the application, object, and interface level in (Col 11 lines 55-60), and the manager can have other accesses. Each control access is a security or policy setting associating with the application, object, and interface level).

12. As per claim 4:

Andrew discloses "Andrew discloses "A system comprising: a pluggable security policy enforcement module configured to be replaceable in the system and to provide different granularities of control for a business logic in the system, wherein the business logic processes requests submitted to the system, wherein the business logic contains problem-solving logic that produces solutions for a particular problem domain" in (Col 7 lines 53-67,

Art Unit: 2135

Col 8 lines 25-50, and Col 14 lines 27-45), and wherein the business logic employs interaction-based definitions in which a component which performs the operation is defined by a series of request-response interaction definitions that can be satisfied to perform the operation" in (Col 7 line 52 to Col 8 line 35), "wherein the pluggable security policy enforcement module includes a control module configured to determine whether to permit an operation based at least in part on accessing the business logic to identify one or more additional tests to perform, and further configured to perform the one or more additional tests" in (Col 11 lines 30-60, and Col 17 lines 43-58).

13. As per claim 5:

Andrew discloses "Andrew discloses "A system as recited in claim 4, wherein the control module is further configured to return a result of the determining to the business logic" in (Col 6 lines 57-65).

14. As per claim 6:

Andrew discloses "A system comprising: a pluggable security policy enforcement module configured to be replaceable in the system and to provide different granularities of control for a business logic in the system, wherein the business logic processes requests submitted to the system, wherein the different granularities of control comprise a plurality of sets of rules, and wherein each set of rules includes a plurality of permission assignment objects" in (Col 7 lines 53-67, Col 8 lines 25-50, and Col 14 lines 27-45), and "wherein the business logic employs interaction-based definitions in which a component which performs the

operation is defined by a series of request-response interaction definitions that can be satisfied to perform the operation” in (Col 7 line 52 to Col 8 line 35),

“wherein each of the permission assignment objects associates a user with a particular role, wherein each particular role is associated with one or more permissions, and wherein each of the one or more permissions identifies a particular operation and context on which the operation is to be performed” in (Col 7 lines 60-67, Col 17 lines 42-65, and Col 11 lines 30-60 (A set of rules associates with each role of many roles. For instance, the user can call the method and can also control access at the application, object, and interface level in (Col 11 lines 55-60), and the manager can have other accesses. Each control access is a security or policy setting associating with the application, object, and interface level).

15. As per claim 7:

Andrew discloses “A system as recited in claim 6, wherein each of the permission assignment objects further identifies whether the one or more permissions in the particular role are granted to the user or denied to the user” in (Col 11 lines 29-60, and Col 17 lines 42-58).

16. As per claim 8:

Andrew discloses “One or more computer-readable media comprising computer-executable instructions that, when executed, direct a processor to perform acts including:



Art Unit: 2135

receiving a request to perform an operation; checking whether to access a business logic in order to generate a result for the requested operation wherein the business logic contains problem-solving logic that produces solutions for a particular, problem domain” in (Col 7 lines 53-67, Col 8 lines 25-50, and Col 14 lines 27-45); and “wherein the business logic employs interaction-based definitions in which a component which performs the operation is defined by a series of request-response interaction definitions that can be satisfied to perform the operation” in (Col 7 line 52 to Col 8 line 35),

“obtaining, from the business logic, a set of zero or more additional tests to be performed in order to generate the result; performing each additional test in the set of tests if there is at least one test in the set of tests;

checking a set of pluggable rules to determine the result of the requested operation;  
and

returning, as the result, a failure indication if checking the business logic or checking the set of pluggable rules indicates that the result is a failure, otherwise returning, as the result, a success indication” in (Col 7 lines 60-67, Col 17 lines 42-65, and Col 11 lines 30-60 (A set of rules associates with each role of many roles. For instance, the user can call the method and can also control access at the application, object, and interface level in (Col 11 lines 55-60), and the manager can have other accesses. Each control access is a security or policy setting associating with the application, object, and interface level).

Art Unit: 2135

17. As per claim 9:

Andrew discloses "One or more computer-readable media as recited in claim 8, wherein the receiving comprises receiving, from the business logic, the request to perform the operation" in (Col 11 lines 29-60, and Col 17 lines 42-58)..

18. As per claim 10:

Andrew discloses "One or more computer-readable media as recited in claim 8, wherein the receiving comprises receiving, as part of the request, an indication of a user, and wherein the checking the set of pluggable rules comprises comparing an object associated with the user to the rules in the set of pluggable rules and determining whether the operation can be performed based at least in part on whether the user is permitted to perform the operation" in (Col 11 lines 29-60, and Col 17 lines 42-58)..

19. As per claim 11:

Andrew discloses "One or more computer-readable media as recited in claim 8, wherein the receiving comprises having one of a plurality of methods invoked" in (Col 11 lines 29-60, and Col 17 lines 42-58).

20. As per claim 12:

Andrew discloses "One or more computer-readable media as recited in claim 8, wherein the set of pluggable rules is a set of security rules defined using high-level permission concepts" in (Col 11 lines 29-60, and Col 17 lines 42-58)..

21. As per claim 13;

Andrew discloses "One or more computer-readable media as recited in claim 12, wherein the high-level permission concepts include an operation and a context, wherein the operation allows identification of an operation to be performed and the context allows identification of what the operation is to be performed on" in (Col 11 lines 29-60, and Col 17 lines 42-58).

22. As per claim 14:

Andrew discloses "One or more computer-readable media as recited in claim 8, wherein the computer-executable instructions are implemented as an object" in (Col 6 lines 57-65).

23. As per claim 15:

Andrew discloses "One or more computer-readable media as recited in claim 8, wherein the computer-executable instructions further direct the processor to perform acts including: determining if at least one of the tests in the set of zero or more additional tests would indicate a result of failure; and returning, as the result, the failure indication without checking the set of pluggable rules" in (Col 11 lines 29-60, and Col 17 lines 42-58).

24. As per claim 16:

Andrew discloses "One or more computer-readable media as recited in claim 8, wherein the set of pluggable rules can be replaced with another set of pluggable rules without altering the business logic" in (Col 7 lines 55-67, Col 11 lines 29-60, and Col 17 lines 42-58).

25. As per claim 17:

Andrew discloses "One or more computer-readable media as recited in claim 8, wherein the set of pluggable rules includes a plurality of permission assignment objects, wherein each of the permission assignment object associates a user with a particular role, wherein each particular role is associated with one or more permissions, and wherein each of the one or more permissions identifies a particular operation and context on which the operation is to be performed" in (Col 11 lines 29-60, and Col 17 lines 42-58).

26. As per claim 18:

Andrew discloses "One or more computer-readable media as recited in claim 17, wherein each of the permission assignment objects further identifies whether the one or more permissions in the particular role are granted to the user or denied to the user" in (Col 11 lines 29-60, and Col 17 lines 42-58).

27. As per claim 19:

Andrew discloses "A method comprising:

providing high-level permission concepts for security rules;

allowing a set of security rules to be defined using the high-level permission concepts,  
wherein the set of security rules allows permissions to be assigned to users of an application;  
and

Art Unit: 2135

determining, based at least in part on a permission assigned to a user, whether to permit an operation based on a request by the user,

wherein the determining further comprises determining whether to permit the operation requested by the user based at least in part on accessing a business logic to the one or more additional tests, wherein the business logic contains problem-solving logic that produces solutions for a particular problem domain" in (Col 11 lines 29-60, and Col 17 lines 42-58). and "wherein the business logic employs interaction-based definitions in which a component which performs the operation is defined by a series of request-response interaction definitions that can be satisfied to perform the operation" in (Col 7 line 52 to Col 8 line 35),

28. As per claim 21:

Andrew discloses "A method as recited in claim 9 further comprising returning a result of the determining to the business logic" in (Col 11 lines 29-60, and Col 17 lines 42-58).

29. As per claim 22:

Andrew discloses "A method as recited in claim 19, wherein the high-level permission concepts include an operation and a context, wherein the operation allows identification of an operation to be performed and the context allows identification of what the operation is to be performed on" in (Col 11 lines 29-60, and Col 17 lines 42-58)..

Art Unit: 2135

30. As per claim 23:

Andrew discloses "A method as recited in claim 19, wherein the method is implemented in an object having a plurality of interfaces for requesting a determination as to whether to permit a plurality of operations including the operation requested by the user" in (Col 11 lines 29-60, and Col 17 lines 42-58).

31. As per claim 24:

Andrew discloses "A method as recited in claim 19, wherein the set of security rules includes a plurality of permission assignment objects, wherein each of the permission assignment objects associates a user with a particular role, wherein each particular role is associated with one or more permissions, and wherein each of the one or more permissions identifies a particular operation and context on which the operation is to be performed" in (Col 11 lines 29-60, and Col 17 lines 42-58).

32. As per claim 25:

Andrew discloses "A method as recited in claim 24, wherein each of the permission assignment objects further identifies whether the one or more permissions in the particular role are granted to the user or denied to the user" in (Col 11 lines 29-60, and Col 17 lines 42-58)..

33. As per claim 26:

Andrew discloses "A method comprising:

receiving a request to perform an operation associated with business logic, wherein the business logic contains problem-solving logic that produces solutions for a particular problem domain" in (Col 7 lines 53-67, and Col 8 lines 25-50), and "wherein the business logic employs interaction-based definitions in which a component which performs the operation is defined by a series of request-response interaction definitions that can be satisfied to perform the operation" in (Col 7 line 52 to Col 8 line 35);

"accessing a set of low-level rules, wherein the low-level rules are defined in terms of high-level concepts;

checking whether a user requesting to perform the operation is entitled to perform the operation based at least in part on the set of low-level rules; and

returning an indication of whether the operation is allowed or not allowed, wherein the set of low-level rules can be replaced with another set of low-level rules without altering the business logic" in (Col 7 lines 60-67, Col 17 lines 42-65, and Col 11 lines 30-60 (A set of rules associates with each role of many roles. For instance, the user can call the method and can also control access at the application, object, and interface level in (Col 11 lines 55-60), and the manager can have other accesses. Each control access is a security or policy setting associating with the application, object, and interface level).

Art Unit: 2135

34. As per claim 27:

Andrew discloses "A method as recited in claim 26, wherein the checking further comprises checking whether the user is entitled to perform the operation based at least in part on accessing the business logic to identify one or more additional tests to perform, and further comprising performing the one or more additional tests" in (Col 7 lines 55-67, Col 11 lines 29-60, and Col 17 lines 42-58).

35. As per claim 29:

Andrew discloses "A method as recited in claim 27, further comprising returning the indication to the business logic" in (Col 7 lines 55-67, Col 11 lines 29-60, and Col 17 lines 42-58).

36. As per claim 30:

Andrew discloses "A method as recited in claim 26, wherein the low-level rules include a plurality of permission assignment objects, wherein each of the permission assignment objects associates a user with a particular role, wherein each particular role is associated with one or more permissions, and wherein each of the one or more permissions identifies a particular operation and context on which the operation is to be performed" in (Col 7 lines 55-67, Col 11 lines 29-60, and Col 17 lines 42-58).

37. As per claim 35:

Andrew discloses "An architecture comprising:

a plurality of resources;



Art Unit: 2135

a business logic layer to process, based at least in part on the plurality of resources, requests received from a client, wherein the business logic layer contains problem-solving logic that produces solutions for particular problem domain, and wherein the business logic employs interaction-based definitions in which a component which performs the operation is defined by a series of request-response interaction definitions that can be satisfied to perform the operation" in (Col 7 line 52 to Col 8 line 35), and

a pluggable security policy enforcement module, separate from the business layer, to enforce security restrictions on accessing information stored at the plurality of resources" in (Col 6 lines 56-65, Col 7 lines 53-67, and Col 8 lines 25-50).

38. As per claim 36:

Andrew discloses "An architecture as recited in claim 35, wherein the pluggable security policy enforcement module defines high-level permission concepts for security rules and further defines a set of security rules using the high-level permission concepts" in (Col 7 lines 55-67, Col 11 lines 29-60, and Col 17 lines 42-58).

39. As per claim 37:

Andrew discloses "An architecture as recited in claim 36, wherein the high-level permission concepts include an operation and a context, wherein the operation allows identification of an operation to be performed and the context allows identification of what the operation is to be performed on" in (Col 7 lines 55-67, Col 11 lines 29-60, and Col 17 lines 42-58).

Art Unit: 2135

40. As per claim 38:

Andrew discloses “An architecture as recited In claim 35, wherein the pluggable security policy enforcement module can be replaced with another pluggable security policy enforcement module to enforce different security restrictions without altering the business logic layer” in (Col 7 lines 55-67, Col 11 lines 29-60, and Col 17 lines 42-58).

41. As per claim 39:

Andrew discloses “An architecture as recited in claim 35, wherein the pluggable security policy enforcement module is configured to determine, based at least in part on a permission assigned to a user and on one or more additional tests identified by accessing the business logic layer, whether to permit an operation to access information at the plurality of resources” in (Col 7 lines 55-67, Col 11 lines 29-60, and Col 17 lines 42-58).

42. As per claim 40:

Andrew discloses “A system as recited in claim 1, wherein the system is configured as a multi-layer architecture, wherein the business logic is implemented as a business logic layer of the multi-layer architecture” in (Col 7 lines 55-67, Col 11 lines 29-60, and Col 17 lines 42-58).

43. As per claim 41:

Andrew discloses “A system as recited in claim 1, wherein the pluggable security policy enforcement module is configured to receive an input from the business logic in

Art Unit: 2135

the form of a user indication and an item indication” in (Col 7 lines 55-67, Col 11 lines 29-60, and Col 17 lines 42-58).

44. As per claim 42:

Andrew discloses “A system as recited in claim 1, wherein the pluggable security policy module includes an interface that provides the following interface functionality: first functionality for testing whether an identified item can be approved by a specified user; second functionality for testing whether the identified item of a specified type can be created by the specified user; third functionality for testing whether the identified item can be deleted by the specified user; fourth functionality -for testing whether the identified item can be modified by the specified user; and fifth functionality for testing whether, the identified user can examine details of the identified item” in (Col 7 lines 55-67, Col 11 lines 29-60, Col 12 lines 47-52, and Col 17 lines 42-58).

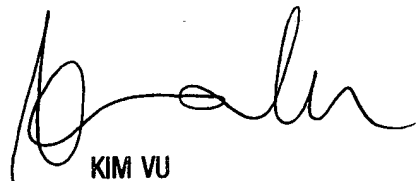
45. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son  
Examiner  
Art Unit 2135



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100